WHAT IS CLAIMED IS:

1. A secure on-line system for printing value bearing items (VBI) comprising:

a client system for interfacing with one or more users; and

a server system capable of communicating with the client system over a communication network comprising:

a secure database remote from the users including information about the users;

computer executable code for password authentication to prevent unauthorized access to the database; and

a cryptographic module for authenticating any of the one or more users.

2. The system of claim 1, wherein the database is accessible through a private network connected to the communication network.

3. The system of claim 2, further comprising a firewall for preventing unauthorized access by a person external to the private network.

4. The system of claim 1, wherein the cryptographic module encrypts transactions related to the database.

5. The system of claim 1, wherein the computer executable code for password authentication comprises of computer executable code for an asynchronous dynamic password verification to terminate a user session if the password authentication fails.

6. The system of claim 1, wherein the database stores a first set of one or more last database transactions and the cryptographic module stores a second set of one or more last database transactions for comparison with the first set of one

or more last database transactions stored in the database to verify each database transaction.

7. The system of claim 6, wherein the cryptographic module prevents further database transactions if the second set of one or more last transaction stored in the cryptographic module does not compare with the first set of one or more last transaction stored in the database.

8. The system of claim 6, wherein the database stores a table including the respective information about a last transaction and a verification module to compare the information saved in the module with the information saved in the database.

9. The system of claim 1, further comprising a back up database server connected to the server system for periodically backing up the data stored in the database in a back up database.

10. The system of claim 9, further comprising a cryptographically protected transaction log stored in the back up database.

11. The system of claim 1, wherein the cryptographic module includes internal registers and the data in the internal registers is cryptographically protected.

12. The system of claim 1, further comprising a plurality of security device transaction data stored in the database for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user.

13. The system of claim 12, wherein the security device transaction data related to a user is loaded into the

cryptographic module when the user requests to operate on a value bearing item.

14. The system of claim 13, wherein the security device transaction data related to a user is updated and returned to the database.

15. The system of claim 13, wherein the security device transaction data related to a user is processed in a stateless manner.

16. The system of claim 1, further comprising at least one more cryptographic module and wherein each cryptographic module is capable of processing data related to any of the one or more users.

17. The system of claim 1, wherein the cryptographic module includes a data validation subsystem to verify that data is up to date and an auto-recovery subsystem for allowing the module to automatically re-synchronize the module with the data.

18. The system of claim 1, wherein the cryptographic module is stateless.

19. The system of claim 1, wherein the cryptographic module includes a computer executable code for preventing unauthorized modification of data.

20. The system of claim 1, wherein the cryptographic module includes a computer executable code for preventing unauthorized disclosure of data.

21. The system of claim 1, wherein the cryptographic module includes a computer executable code for ensuring the proper operation of cryptographic security and VBI related meter functions.

22. The system of claim 1, wherein the cryptographic module includes a computer executable code for detecting errors and preventing a compromise of data or critical cryptographic security parameters as a result of the errors.

23. The system of claim 1, wherein the cryptographic module includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

24. The system of claim 1, wherein the database includes one or more indicium data elements, data for account maintenance, and data for revenue protection.

25. The system of claim 1, wherein the database includes a private key associated with a user.

26. The system of claim 1, wherein the database includes virtual meter information.

27. The system of claim 1, wherein the database includes ending registers data.

28. The system of claim 1, wherein the value bearing item is a mail piece.

29. The system of claim 28, wherein the mail piece includes a digital signature.

30. The system of claim 1, wherein the cryptographic module performs cryptographic function on validation information according to a user request for printing a VBI.

31. The system of claim 1, wherein the cryptographic module generates data sufficient to print a postal indicium in compliance with postal service regulation on a mail piece.

32. The system of claim 1, wherein the value bearing item is a ticket.

33. The system of claim 1, wherein a bar code is printed on the value bearing item.

34. The system of claim 1, wherein the value bearing item is a coupon.

35. The system of claim 1, wherein the value bearing item is currency.

36. The system of claim 1, wherein the value bearing item is a voucher.

37. The system of claim 1, wherein the value bearing item is a traveler's check.

38. The system of claim 12, wherein each security device transaction data includes one or more of an ascending register value, a descending register value, a respective cryptographic module ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client

subsystem, an operational state of the respective module, expiration dates for keys, and a passphrase repetition list.

39. The system of claim 12, wherein the database includes a private key associated with a user.

40. The system of claim 12, wherein each security device transaction data includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign module status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the module and the VBI are authentic.

41. The system of claim 1, wherein the cryptographic module is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

42. The system of claim 1, wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address matching service subsystem, a SSL proxy server subsystem, and a web server subsystem.

43. The system of claim 1, wherein the database includes one or more of a postal database, a provider database, an e-commerce database, an affiliate database, a website database and a membership database.

44. The system of claim 1, further comprising an offline database for storing one or more postal transaction data,

financial transaction data, customer marketing information, commerce product information, meter license information, meter resets, meter history, and meter movement information.

45. The system of claim 1, further comprising a data warehouse database for storing customer information, financial transactions, and information for marketing queries.

46. The system of claim 1, further comprising a commerce database including one or more payment databases, an e-mail database, and a stamp mart database.

47. The system of claim 1, further comprising an e-commerce server for authorizing and capturing funds from a customer's account and transferring the funds to a vendor's account.

48. The system of claim 1, further comprising an address matching server for verifying a correct address specified by a user.

49. The system of claim 1, further comprising a printer driver database for storing supported printer driver information.

50. A method for securely printing value-bearing items (VBI) via a communication network including a client system and a server system, the method comprising the steps of:

interfacing with one or more users via the client system;

communicating with the client system over the communication network;

storing user information in a secure database accessible through the communication network;

preventing unauthorized access to the database by users external to the communication network; and

authenticating one or more users using a cryptographic module.

51. The method of claim 50, further comprising the step of encrypting database transactions by the cryptographic module.

52. The method of claim 50, further comprising the steps of

storing one or more last database transactions in the database;

storing one or more last database transactions in the cryptographic module; and

comparing the one or more last database transactions stored in the database with the one or more last database transactions stored in the cryptographic module to verify each database transaction.

53. The method of claim 50, further comprising the step of preventing unauthorized access by a person external to the private network using a firewall.

54. The method of claim 50, further comprising the step of encrypting transactions related to the database by the cryptographic module.

55. The method of claim 50, further comprising the steps of storing one or more last database transactions in the database, storing one or more last database transactions in the cryptographic module for comparison with the one or more last database transactions stored in the database to verify each database transaction.

56. The method of claim 55, further comprising the step of preventing further database transactions if the one or more last transaction stored in the cryptographic module does not compare with the one or more last transaction stored in the database.

57. The method of claim 50, further comprising the step of storing a table including the respective information about a last transaction and comparing the information saved in the module with the information saved in the database.

58. The method of claim 50, further comprising the step of backing up data stored in the database in a back up database.

59. The method of claim 58, further comprising the step of recovering data from the back up database by decrypting an encrypted transaction log stored in the back up database.

60. The method of claim 50, further comprising the step of cryptographically protecting data in the internal registers of the cryptographic module.

61. The method of claim 50, further comprising the step of storing in the database a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user.

62. The method of claim 61, further comprising the step of loading into the cryptographic module a security device transaction data related to a user when the user requests to operate on a value bearing item.

63. The method of claim 62, further comprising the steps of updating and returning to the database the security device transaction data related to a user after the user request is completed.

64. The method of claim 63, further comprising the steps of preventing unauthorized modification of data by the cryptographic module.

65. The method of claim 50, further comprising the steps of verifying that the database is up to date.

66. The method of claim 65, further comprising the steps of automatically re-synchronizing the cryptographic module with the database.

67. The method of claim 50, further comprising the step of preventing unauthorized display of data.

68. The method of claim 50, further comprising the step of ensuring the proper operation of cryptographic security and VBI related meter functions.

69. The method of claim 52, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.

70. The method of claim 50, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database;

comparing the information saved in the respective device with the respective information saved in the database; and

loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

71. The method of claim 50, further comprising the step of storing data for creating an indicium, account maintenance, and revenue protection.

72. The method of claim 50, further comprising the step of printing a mail piece.

73. The method of claim 72, wherein the mail piece includes a digital signature.

74. The method of claim 72, wherein the mail piece includes a postage amount.

75. The method of claim 72, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

76. The method of claim 50, further comprising the step of printing a ticket.

77. The method of claim 50, further comprising the step of printing a bar code.

78. The method of claim 50, further comprising the step of printing a coupon.

79. The method of claim 50, further comprising the step of printing currency.

80. The method of claim 50, further comprising the step of printing a voucher.

81. The method of claim 50, further comprising the step of printing a traveler's check.

82. The method of claim 61, wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

83. The method of claim 50, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms by each of the cryptographic devices.

84. The method of claim 50, further comprising the step keeping track of user accesses to a vendor website by a website database.

85. The method of claim 50, further comprising the step of storing postal transactions data, financial transaction data, customer marketing information, commerce product information,

meter license information, meter resets, meter history, and meter movement information in an offline database.

86. The method of claim 50, further comprising the step of storing customer information, financial transactions, and information for marketing queries in a data warehouse database.

87. The method of claim 50, further comprising the steps of authorizing and capturing funds from a customer's account and transferring the funds to a vendor's account by an e-commerce server.

88. The method of claim 50, further comprising the step of verifying a correct address specified by a user using an address matching server.

89. The method of claim 50, further comprising the step of storing supported printer driver information in a printer driver database.

90. The method of claim 50, further comprising the step of verifying a user password before granting access to the database.

91. The method of claim 50, further comprising the step of storing a private key associated with a user in the secure database.

92. An on-line system for printing value bearing items (VBI) comprising:

a client system for interfacing with one or more users;

a server system capable of communicating with the client system over a communication network comprising:

a first database remote from the user including information about the user;

a cryptographic module for authenticating any of the one or more users; and

a backup database server connected to the server system for backing up data in a back up database.

93. The system of claim 92, further comprising a cryptographically protected transaction log stored in the back up database for recovering data from the back up database.

94. The system of claim 92, wherein the first database is accessible through a private network connected to the communication network.

95. The system of claim 92, further comprising a firewall for preventing unauthorized access by a person external to the private network.

96. The system of claim 92, wherein the cryptographic module encrypts transactions related to the database.

97. The system of claim 92, wherein the cryptographic module includes internal registers and the data in the internal registers is cryptographically protected.

98. The system of claim 92, further comprising a plurality of security device transaction data stored in the database for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user.

99. The system of claim 98, wherein the security device transaction data related to a user is loaded into the cryptographic module when the user requests to operate on a value bearing item.

100. The system of claim 99, wherein the security device transaction data related to a user is updated and returned to the database after the user request is completed.

101. The system of claim 92, wherein the value bearing item is a mail piece.

102. The system of claim 101, wherein the mail piece includes a digital signature.

103. The system of claim 92, wherein the cryptographic module encrypts validation information according to a user request for printing a VBI.

104. The system of claim 92, wherein the cryptographic module generates data sufficient to print a postal indicium in compliance with postal service regulation on a mail piece.

105. The system of claim 92, wherein the value bearing item is a ticket.

106. The system of claim 92, wherein a bar code is printed on the value bearing item.

107. A method for printing value-bearing items (VBI) via a communication network including a client system and a server system, the method comprising the steps of:

interfacing with one or more users via the client system;

communicating with the client system over the communication network;

storing user information in a database accessible through the communication network;

authenticating the users by a cryptographic module; and

backing up data stored in the database in a back up database.

108. The method of claim 107, further comprising the step of recovering data from the back up database by decrypting an encrypted transaction log stored in the back up database.

109. The method of claim 107, further comprising the step of encrypting database transactions by the cryptographic module.

110. The method of claim 107, further comprising the steps of

storing one or more last database transactions in the database;

storing one or more last database transactions in the cryptographic module; and

comparing the one or more last database transactions stored in the database with the one or more last database transactions stored in the cryptographic module to verify each database transaction.

111. The method of claim 107, further comprising the step of preventing unauthorized access by a person external to the private network using a firewall.

112. The method of claim 107, further comprising the step of encrypting transactions related to the database by the cryptographic module.

113. The method of claim 107, further comprising the steps of storing one or more last database transactions in the database, storing one or more last database transactions in the cryptographic module for comparison with the one or more last database transactions stored in the database to verify each database transaction.

114. The method of claim 113, further comprising the step of preventing further database transactions if the one or more last transaction stored in the cryptographic module does not compare with the one or more last transaction stored in the database.

115. The method of claim 107, further comprising the step of storing data for creating an indicium, account maintenance, and revenue protection.

116. The method of claim 107, further comprising the step of printing a mail piece.

117. The method of claim 116, wherein the mail piece includes a digital signature.

118. The method of claim 116, wherein the mail piece includes a postage amount.

119. The method of claim 116, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

120. The method of claim 107, further comprising the step of printing a ticket.

121. The method of claim 107, further comprising the step of printing a bar code.